Federal Bridge Certification Authority (BCA) Border Directory System Proposal

Dave Fillingham

5 January 1998

Background and Problem Introduction

The Federal Public Key Infrastructure Technical Working Group (FPKITWG) has developed the Bridge Certification Authority (BCA) concept to provide certificate chains to link "enterprise" Public Key Infrastructures (PKIs) within the Federal government, and to provide trust chains between the Federal Public Key Infrastructure (FPKI) and those of external organizations, like our allies and commercial partners. While the BCA concept provides a necessary component for a Federal PKI, it does not, at present, provide a complete PKI solution. The existence of certificate chains among infrastructures does not, by itself, provide the ability for subscribers of different PKIs to communicate securely. In particular, the BCA concept as defined to date does not provide a mechanism for making certificates or revocation information generated in any given public key infrastructure domain available to relying parties in other public key infrastructure domains. For example, if the Treasury Department and the Department of Defense (DoD) were to cross-certify with the BCA, a trust chain would exist between the subscribers of both infrastructures, but the Treasury Department relying parties would have no automated mechanism to obtain the public key certificates issued within the DoD, nor would the DoD relying parties have an automated mechanism to obtain public key certificates issued by the Treasury department. There is a similar problem with sharing revocation information, such as Certificate Revocation Lists (CRLs), between PKIs. It is not clear how cross-certificates issued by the BCA and posted to the BCA repository would be made available to relying parties, since the mere existence of a BCA repository is not enough to make its contents available. Technical mechanisms must be implemented that would allow Federal relying parties to access the BCA repository. In the absence of automated mechanisms to share certificates and revocation information among BCA subscribers, the cross-certificates issued by the BCA offer little practical value.

This paper describes the concept of Border Directory System Agents (BDSAs). A Directory System Agent (DSA) is a server that provides directory services to end entity clients. A BDSA is a DSA intended to provide directory services to users outside an agency. BDSAs are intended to allow seamless interoperation among BCA cross-certified subscribers. The BDSA concept was originally developed by the Combined Communications Electronics Board (CCEB) nations in support of efforts to achieve interoperation among allied military certificate management infrastructures. It seems possible that this concept might be adapted to use within the Federal government.

Philosophical Underpinnings

The BDSA concept was developed to follow the "bottom up" design philosophy that has made the BCA concept attractive. The "bottom up" Federal PKI approach assumes that Certificate Management Infrastructures (CMI's) will be deployed throughout the Federal

government by different agencies and departments in response to local requirements. Over time, we expect that these local CMIs will be integrated into a larger Federal CMI when department and agency managers see such integration as being practical and valuable. This approach contrasts with a "top down" approach in which the Federal government would develop a comprehensive CMI design, and require local departments and agencies to procure public key systems that conform to Federal standards so as to "fit in" to the Federal CMI architecture.

Assumptions Regarding Existing Directories and Repositories

The "bottom up" approach assumes that many "local" Federal CMI's already exist, and that each implements some form of directory system (or "repository system"). Because these systems are procured from diverse vendors by diverse agencies in support of diverse requirements, we can assume that these directories/repositories:

- will use a mix of protocol standards such as Directory Access Protocol (DAP), Lightweight Directory Access Protocol (LDAP) of various versions, and even proprietary protocols for client access to the local directories;

- will only be oriented toward sharing data between DSAs or repositories within their agency domain. As a result, many department and agency DSAs will implement proprietary mechanisms for sharing information among themselves, or they will implement incompatible versions of standard protocols, such as the X.500 Directory System Protocol.

Furthermore, the contents of local DSAs/repositories may not be appropriate for sharing with the world at large. A local agency DSA/repository may include information on every Federal employee within that agency/department. Such complete directories might be appropriate if access to the repository is restricted to agency/department intranet users. For privacy, or other local policy reasons, it may be inappropriate to make the "intranet accessible" DSAs available to the general public.

Requirements and Goals

In order for the Border DSA concept to be feasible, it should, to the extent possible, meet the following requirements and goals:

Make Necessary PKI Data Available - The primary requirement for the BDSA system is to make public key certificates and revocation information issued by any BCA subscriber infrastructure, or by the BCA itself, transparently available to clients of the subscriber infrastructures.

Not impact client applications - client applications are in-place, and performing functions critical to existing government operations. Often, they are customized to meet specific local requirements. Any approach that would require client applications to be replaced or modified would be viewed as infeasible.

Maximize User "Transparency" - ideally, the matter of integrating the subscribers of a "local" PKI into the Federal BCA community would be completely transparent to the users. Users already have their clients configured to access their local DSA/repository. The Border DSA concept should not require users to reconfigure their client applications to access some other device.

Minimize Impacts to Local Infrastructure Directory/Repository and PKI Systems - An approach that required all Federal users to standardize on a new Directory/Repository system would probably be infeasible. The Border DSA system should allow existing Directory/Repository systems to remain in-place.

Allow Many Different Vendors to Provide Directory/Repository Services to the Federal Government - An approach that relied upon capabilities that are only available from a small set of DSA vendors would probably be seen as unfair, and would slow - or even prevent - implementation.

Provide Segregation of Directory/Repository Data between that Accessible by Intranet and Internet - An approach that would require participating departments and agencies to make the entire content of their intranet-accessible directories/repositories available to the Internet would almost certainly be unacceptable. The BDSA concept should provide strong assurance that only appropriate entries and attributes are available to the "world at large" based on local policies.

Border Directory System Agent Description

The BDSA concept requires each "local" BCA subscriber infrastructure (that is, a PKI that has cross-certified with the BCA) provide one or more Border Directory System Agents to interact with a Federal BDSA network. The BDSA would act as the subscriber infrastructure's "face to the world." The BDSA would obtain the appropriate information from the subscriber PKI, and provide it to the Federal network of BDSAs. The BDSA would also serve the reverse function, of responding to queries from the subscriber PKI clients for certificates and revocation information from the Federal BDSA network.

Subscribers would continue to query their local intranet DSA for any certificates or CRLs, regardless of whether the query was associated with an attempt to obtain the certificate or CRL of a local PKI subscriber or of a cross-certified PKI subscriber. It would be a responsibility of the local DSA to query the border DSA when that is necessary to respond to the subscriber's request, and it would then be a responsibility of the Border DSA to query the Federal BDSA network to obtain the necessary information. Alternatively, where local clients support referral mechanisms, the local DSA could refer local clients to the Border DSA for external certificates and CRLs.

The functional interfaces for the BDSA can be illustrated like this:

[Subscriber PKI & Clients] <--->[Border DSA]<--->[Federal Border DSA System]

There is considerable flexibility in how the interface between the Subscriber PKI and the Border DSA can be implemented. In every case, though, the kinds of information that traverses the interface is the same.

Subscriber PKI to Border DSA

The subscriber PKI must place "appropriate" subscriber certificates and revocation information into the Border DSA. This can be done in one of two ways, and each mechanism will likely be used according to local circumstances.

- **Replication** - Replication is an X.500 mechanism that allows information from one DSA to be selectively reproduced in another DSA according to "shadowing agreements" made between the DSAs. In this implementation, the administrator of the intranet DSA associated with the subscriber PKI would configure the intranet DSA to provide appropriate certificates and revocation data to the Border DSA. This approach has the advantage of being more or less "automatic" once the shadowing agreements are in place, but has the disadvantage of requiring a replication capability in the internal DSAs - and this is a capability many will not have unless upgrades or replacement of local DSA/Repositories are undertaken. While X.500 provides a standard protocol for performing this function, it is not necessary that the FPKI specify use of X.500 or any other protocol for this interface. Proprietary protocols are acceptable, so long as the internal and Border DSAs can communicate to perform the necessary function.

- **Selective PKI Population** of the Border DSA - the Certification Authorities (CAs) within the subscriber PKI could selectively post subscriber information to the Border DSA. In other words, the subscriber PKI CAs could post all subscriber certificates and CRLs to the intranet Directory/Repository system (as they always have), but could also post appropriate certificates and CRLs for use by the "outside world" to the BDSA. This approach does not add any requirements to the internal DSAs, and should be implementable with any DSA/Repository that can interface to existing CA tools. On the other hand, it requires the CAs to correctly post certain subscribers' certificates to both the BDSA and the intranet DSA/Repository, and to post other subscribers' certificates only to the intranet DSA/Repository. Again, there is no need for the Federal PKI to standardize the protocols used on this interface.

In addition to the certificates and CRLs flowing from the Internal PKI to the Border DSA, the BDSA will receive queries from the subscriber PKI users for "external" certificates and CRLs. These queries may take place via the intranet DSA (though X.500 chaining or similar mechanisms) or they may be made directly by the intranet subscribers by LDAP referrals. Once more, there is no need for the Federal PKI to standardize protocol implementations on this interface.

Border DSA to Subscriber PKI

The BDSA will transfer "external" certificates and CRLs to the subscriber PKI clients - either through the intranet DSA/Repository via a chaining mechanism, or directly by means of LDAP referrals (or, conceivably, proprietary mechanisms could be used). As long as the function is performed, there is no need for the Federal government to attempt to standardize the mechanism.

Border DSA to Border DSA System

The Border DSA is responsible for obtaining "external" certificates and CRLs from the Federal Border DSA system, and for providing appropriate certificates and CRLs to that system. This will be accomplished using X.500 Directory System Protocol "chaining" among the Federal Border DSAs. The intra-Border DSA interfaces must be standardized.

Need for Standards

The standards necessary to implement the BDSA concept include:

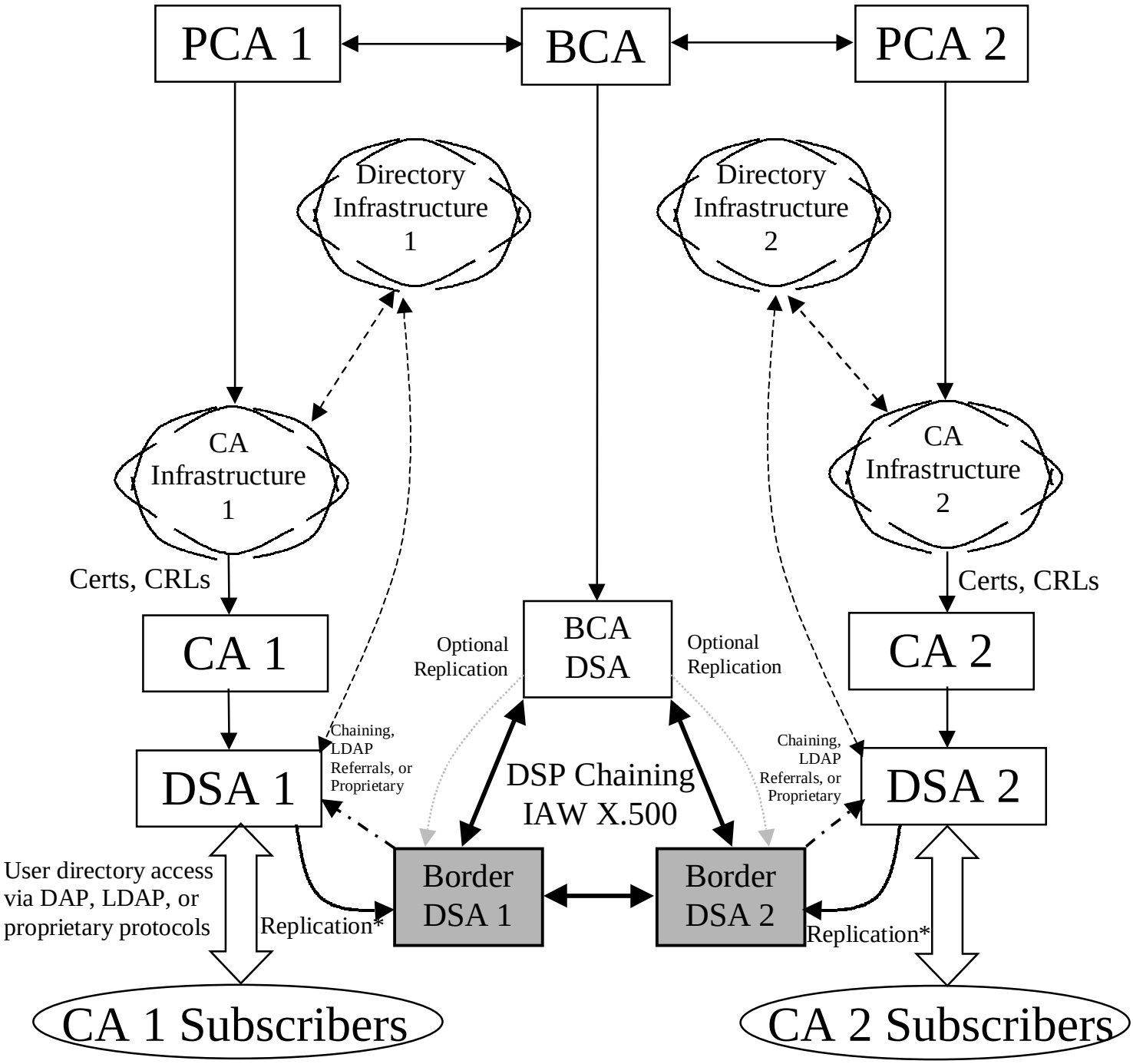
Minimum Schema - The matter of what information is to be made available in the BDSAs, in what attributes, and using what syntax, needs to be standardized among Federal BDSA implementations. The Internet Engineering Task Force/PKIX committee has proposed an LDAP V2 schema which has already been vetted by industry, so it may be a strong candidate for a BDSA implementation.

Knowledge Management - A Directory Information Tree for the BDSA would need to be implemented so BDSAs could direct their queries to the correct external BDSAs within the BDSA network.

There may be other standards required as well, dealing with matters such as time synchronization.

Acknowledgement

I would like to thank Bill Burr of the National Institute of Standards and Technology for his review, comments and contributions to this paper.



* Note: An alternative to replication of data from the intranet DSAs to the Border DSAs is to have CAs selectively post data to the Border DSAs.

Acronyms

BCA	Bridge Certification Authority
PCA	Principal Certification Authority
CA	Certification Authority
DSA	Directory System Agent

Figure One
The Federal Border Directory System Agent Concept